The Bounded Storage Model in The Presence of a Quantum Adversary

Robert König[1] and Barbara M. Terhal[2]

[1] *Centre for Quantum Computation, DAMTP, University of Cambridge, Cambridge CB3 0WA, UK and*

[2]*IBM Watson Research Center, P.O. Box 218, Yorktown Heights, NY 10598, USA*
(Dated: February 1, 2008)

An extractor is a function E that is used to extract randomness. Given an imperfect random source X and a uniform seed Y, the output $\mathsf{E}(X,Y)$ is close to uniform. We study properties of such functions in the presence of prior quantum information about X, with a particular focus on cryptographic applications. We prove that certain extractors are suitable for key expansion in the bounded storage model where the adversary has a limited amount of quantum memory. For extractors with one-bit output we show that the extracted bit is essentially equally secure as in the case where the adversary has classical resources. We prove the security of certain constructions that output multiple bits in the bounded storage model.

I. INTRODUCTION

The aim of *randomness extraction* is to generate "almost uniform" randomness given an imperfect source of randomness X. The term "extractor" is generally used to describe a procedure which accomplishes this task; more formally, an extractor is a (deterministic) function $\mathsf{E} : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ which, when applied to an imperfect source X and a uniform and independent seed Y, yields an output $Z := \mathsf{E}(X,Y)$ which is close to being uniformly distributed on $\mathcal{Z}$. Such an extractor is characterized by a number of parameters. Among these are the amount of randomness Y that is required, the amount of randomness Z produced, and, most importantly, the character of the sources X which lead to almost uniform output. A very general class of sources are the *weak* sources X, characterized by a lower bound on the *min-entropy* $H_\infty(X) := -\log \max_x P_X(x)$. Correspondingly, a (k, ε)-extractor [1] commonly refers to an extractor which, for any input distribution P_X with $H_\infty(X) \geq k$, outputs ε-uniform randomness Z.

Besides purifying randomness, extractors are an essential tool in computer science, in particular in complexity theory and cryptography. Correspondingly, the study of such extractors has been a major research topic in recent years, and much understanding has been gained (see [2] for a review). For applications in computer science, the challenge is to find explicit, efficiently computable extractors with good parameters.

In a cryptographic context, a certain variant of the concept of a (k, ε)-extractor is of particular importance. These are called *strong* extractors; they have the additional property that even the pair $(Y, \mathsf{E}(X,Y))$ is ε-close to uniform. This means for example that $(Y, \mathsf{E}(X,Y))$ can be used to encrypt a message $M = (M_1, M_2)$ using a one-time pad [3] as $C = (C_1, C_2) = (M_1 \oplus Y, M_2 \oplus \mathsf{E}(X,Y))$. An adversary who learns the cipher-text C as well as the message M_1 (and thus the seed Y) will be completely ignorant of the content of the remaining message M_2. Expressed differently, the pair $(Y, \mathsf{E}(X,Y))$ is

a key with *universally composable* security [4, 5].

A more striking application of strong extractors in cryptography is privacy amplification, introduced by Bennett, Brassard and Robert [6] and further analyzed in [7]. This refers to a technique that allows two parties, Alice and Bob, to generate a secret key Z from a shared random variable X about which the adversary has partial information E. The only assumption is that the parties are connected by an authentic but otherwise completely insecure channel. The key Z is then obtained as follows: Alice generates an independent uniform seed Y and sends it over the channel. Subsequently, both parties apply a strong extractor to get $Z := \mathsf{E}(X,Y)$. The security of Z when used as a secret key directly follows from the properties of the strong extractor, assuming a certain bound on the information E of the adversary.

Apparently related to privacy amplification, but conceptually quite different, is Maurer's bounded storage model [8]. The first security proof for general adversaries in this model was obtained by Aumann, Ding and Rabin [9] and essentially optimal constructions were subsequently found in a sequence of papers [10, 11, 12]. Its aim is not *key extraction*, but *key expansion*. In this setting a large amount of randomness X is publicly, but only temporarily available. Alice and Bob use a previously shared (short) secret key Y to obtain additional key bits $Z = \mathsf{E}(X,Y)$ using a strong extractor. The seed Y remains hidden to the adversary until (possibly) after the execution of the protocol. The adversary is assumed to have only a bounded amount of storage (which may be much larger than the honest parties' memory). As a result, his information E about X is limited, once X becomes inaccessible, and by the properties of the extractor, Z can be shown to be secure even if he later obtains the seed Y (this was referred to as "everlasting security" in [9]).

From a cryptographic viewpoint, a natural generalization of these scenarios is arrived at by allowing the adversary to have quantum information Q instead of only classical information E about X. This modification is

not merely of theoretical interest. Indeed, the only construction proved to be secure [13, 14, 15, 16] for privacy amplification has found various applications in quantum cryptography. Besides simplifying and improving security proofs for quantum key distribution [16, 17], the quantum version of privacy amplification has been used to derive both possibility [18] and impossibility [19] results for tasks such as bit commitment or oblivious transfer.

While the problem of constructing strong extractors is well-studied, little is known about the security resulting from their use in a quantum context. For the bounded storage model, Gavinsky, Kempe and de Wolf [20] recently gave an example of an extractor which yields a classically secure key, but is completely insecure against an adversary with a similar amount of quantum storage. There is no construction for the bounded storage model that is known to be secure against a quantum adversary.

In this paper, we study properties of strong extractors in a context where the adversary has quantum information, with the two cryptographic settings described in mind. We give the first constructions of extractors that are usable in the bounded storage model against a quantum adversary, and we show that certain strong extractors generate secure key bits in the setting of privacy amplification. This allows to reduce the amount of communication needed in certain applications. Our constructions achieve the most desirable type of security, that is, the extracted keys are *universally composable* [15, 21, 22].

Outline

In Section II we introduce the relevant definitions. In Section III we show that any strong extractor which outputs a single bit yields essentially the same degree of security in a cryptographic setting, irrespective of whether the adversary has quantum or classical information. We then use a hybrid argument in Section IV to obtain extractors that output several bits. In Section V we explain how these extractors can be used in the bounded storage model. Finally, we show that general strong extractors can be used in the setting of privacy amplification in Section VI. We conclude in Section VII.

A. Notation

Throughout this paper, all logarithms are binary, i.e., to base 2. For a random variable X with range $\mathcal{X}$, we define the *min-entropy* of X as $H_\infty(X) := -\log \max_x P_X(x)$. More generally, for a quantum state ρ_Q on a Hilbert space $\mathcal{Q}$, $H_\infty(Q)$ is the min-entropy of the distribution of eigenvalues of ρ_Q. Analogously, the max-entropy is defined as $H_0(X) := \log |\mathrm{supp}(P_X)| = \log |\mathcal{X}|$ and $H_0(Q) := \log \mathrm{rank}(\rho_Q)$, respectively. Expressed differently, $H_0(Q)$ is the number of qubits constituting sys-

tem Q. For a function $g : \mathcal{X} \to \mathbb{R}$, we denote by

$$\mathbb{E}_{x \leftarrow P_X}[g(x)] := \sum_{x \in \mathcal{X}} P_X(x)g(x)$$

the expectation of $g(X)$ over a random choice of $x \leftarrow P_X$. We also use the notation $P_X \cdot P_Y$ to refer to the joint distribution of two independent random variables X and Y, that is, $\Pr[X = x, Y = y] = P_X(x) \cdot P_Y(y)$ for all $(x, y) \in \mathcal{X} \times \mathcal{Y}$.

In the sequel, Q refers to a quantum system, whereas E, V, W, X, Y and Z are assumed to be classical. Slightly abusing notation, we sometimes refer to the Hilbert space corresponding to a classical-quantum state (cq-state) ρ_{XQ} by $\mathcal{X} \otimes \mathcal{Q}$. We denote the completely mixed state on $\mathcal{X}$ by $\rho_{\mathcal{U}_{\mathcal{X}}}$.

We will sometimes use classical-quantum states with multipartite classical parts, e.g., a ccq-state ρ_{XYQ}. For such a state ρ_{XYQ}, we say that $Y \leftrightarrow X \leftrightarrow Q$ forms a Markov chain if it has the form

$$\rho_{XYQ} = \sum_{x,y} P_{XY}(x,y)|xy\rangle\langle xy| \otimes \rho_x \qquad (1)$$

for some states $\{\rho_x\}_{x \in \mathcal{X}}$ on $\mathcal{Q}$. A state with this property defines a distribution P_{XY}, which defines the conditional distributions $P_{X|Y=y}$ and, for any function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$, the distribution $P_{f(X,Y)XY}$. The corresponding conditional states $\rho_{XQ|Y=y}$ are obtained by making the approriate replacement in Eq. (1), i.e.,

$$\rho_{XQ|Y=y} = \sum_x P_{X|Y=y}(x)|x\rangle\langle x| \otimes \rho_x \ .$$

Similarly, we can define the cccq-state

$$\rho_{f(X,Y)XYQ} = \sum_{x,y} P_{XY}(x,y)|f(x,y)xy\rangle\langle f(x,y)xy| \otimes \rho_x \ ,$$

which in turn gives rise to states such as $\rho_{f(X,y)XQ|Y=y}$.

We will use the trace norm $\|A\| := \frac{1}{2}\mathrm{tr}(\sqrt{A^\dagger A})$ for any operator A. Note that if ρ_{XQ} and $\sigma_{X'Q'}$ are cq-states on $\mathcal{X} \otimes \mathcal{Q}$, then

$$\|\rho_{XQ} - \sigma_{X'Q'}\| = \sum_{x \in \mathcal{X}} \|P_X(x)\rho_x - P_{X'}(x)\sigma_x\| \ . \qquad (2)$$

For two probability distributions P and Q on $\mathcal{X}$, the trace norm of their difference (when identifying the distribution with a state), i.e. $\|P - Q\| := \frac{1}{2}\sum_{x \in \mathcal{X}} |P(x) - Q(x)|$ is also known as the variational distance.

Let $\rho_{XQ} = \sum_{x \in \mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \rho_x$ be a cq-state. Consider a fixed POVM $\mathcal{E} := \{E_z\}_{z \in \mathcal{Z}}$ on $\mathcal{Q}$. We denote by $P_{XZ} \equiv \rho_{X\mathcal{E}(Q)}$ the joint distribution of X and the measurement outcome, i.e.,

$$P_{Z|X=x}(z) = \mathrm{tr}(E_z\rho_x)$$

for every $z \in \mathcal{Z}$ and $x \in \mathcal{X}$.

We will often encounter scalar quantities d that are functions of a given distribution or a quantum state, i.e., $d = d(P_X)$ or $d = d(\rho_Q)$. In these cases, we use the shorthand $d(X)$ or $d(Q)$. Similarly, we write $d(Q|W = w)$ instead of $d(\rho_{Q|W=w})$. More generally, we will consider quantities that depend on a specific bipartition of a state ρ_{ZE} into Z and E; in these cases, we write $d(Z \leftarrow E)$. Again, we use the notation $d(Z \leftarrow E|W = w)$ to denote the corresponding quantity for the conditional state $\rho_{ZE|W=w}$.

II. EXTRACTORS AND SECRET KEYS

A. Classical adversaries

Before reviewing the definition of strong extractors and various of their basic properties, let us introduce a shorthand notation for the *non-uniformity*, a quantity which measures the extent to which a probability distribution of a random variable Z deviates from the uniform distribution, possibly given another random variable E:

Definition 1. *Let P_{ZE} be an arbitrary distribution. The non-uniformity $d(Z \leftarrow E)$ of Z given E is defined as*

$$d(Z \leftarrow E) := \|P_{ZE} - P_{\mathcal{U}_z} \cdot P_E\|.$$

Here P_E is the marginal distribution of P_{ZE}, and $P_{\mathcal{U}_z}$ denotes the uniform distribution on $\mathcal{Z}$.

Note that $d(Z)$ is simply the distance of the distribution P_Z from the uniform distribution. A strong extractor can then be defined as follows.

Definition 2. *A* strong (k, ε)-extractor *is a function* $\mathsf{E} : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ *with the property that*

$$d(\mathsf{E}(X, Y) \leftarrow Y) = \|P_{\mathsf{E}(X,Y)Y} - P_{\mathcal{U}_z} \cdot P_{\mathcal{U}_y}\| \leq \varepsilon \quad (3)$$

for all distributions P_X with $H_\infty(X) \geq k$. Here Y is independent of X and uniformly distributed on $\mathcal{Y}$.

The definition implies that $\mathsf{E}(X, y)$ is close to being uniformly distributed on $\mathcal{Z}$ on average over the random choice of $y \leftarrow P_Y$ (cf. Eq. (A3)). In other words, if X is chosen according to P_X and Y is uniformly distributed and independent of X, then $\mathsf{E}(X, Y)$ is indistinguishable from uniform, even given Y.

In a cryptographic setting, the security of the extracted key $Z := \mathsf{E}(X, Y)$ with respect to an adversary who is given Y is exactly characterized by Eq. (3). Indeed, expression (3) quantifies how distinguishable the real system (consisting of (Z, Y)) is from the ideal system, in which Z is uniformly distributed and independent of Y. This is easily generalized to a setting where the adversary is given additional information about X. The additional information can be in the form of a classical random variable (i.e., bits) that is jointly distributed with X or a quantum state (i.e., qubits).

In case the adversary has classical information about X expressed by a random variable E, one can show that this simply reduces the min-entropy of X. If E gives little information about X it follows that even given E and Y, the extracted bits look random. This intuition is made explicit in the following proposition (all proofs in this section can be found in Appendix B):

Proposition 1. *Let $\mathsf{E} : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a strong (k, ε)-extractor. Let P_{XE} be a distribution with*

$$H_{\mathsf{g}}(X \leftarrow E) \geq k + \log 1/\varepsilon . \quad (4)$$

Here the guessing-entropy $H_{\mathsf{g}}(X \leftarrow E)$ of X given E is defined as

$$H_{\mathsf{g}}(X \leftarrow E) := -\log \max_{\hat{X}} \Pr[X = \hat{X}] ,$$

where the maximum is taken over all random variables $\hat{X}$ such that $X \leftrightarrow E \leftrightarrow \hat{X}$ forms a Markov chain. Then

$$d(\mathsf{E}(X, Y) \leftarrow YE) \leq 2\varepsilon ,$$

where $P_{YXE} := P_{\mathcal{U}_y} \cdot P_{XE}$.

Note that if E is trivial or independent of X the guessing entropy $H_{\mathsf{g}}(X \leftarrow E)$ of X given E is equal to the min-entropy $H_\infty(X)$ of X. Proposition 1 can be applied in the bounded storage model because the limitation on the adversary's storage implies that his information about X is bounded. More precisely, the guessing probability has the following intuitive property. Any (additional) piece of information W does not increase the success probability in guessing by a significant amount if the size of W is small. More trivially, independent information V does not affect the guessing probability. We express this formally in Lemma 1; versions of this statement are implicit in [1], and more explicitly given in [23].

Lemma 1. *Consider a distribution P_{XVWE} with $P_{XV} = P_X \cdot P_V$ and $VW \leftrightarrow X \leftrightarrow E$. Then*

$$H_{\mathsf{g}}(X \leftarrow VWE) \geq H_{\mathsf{g}}(X \leftarrow E) - H_0(W) .$$

In particular, for every $\varepsilon \geq 0$,

$$H_{\mathsf{g}}(X \leftarrow E|V = v, W = w) \geq H_{\mathsf{g}}(X \leftarrow E) - H_0(W) - \log 1/\varepsilon$$

with probability at least $1 - \varepsilon$ over $(v, w) \leftarrow P_{VW}$.

B. Quantum adversaries

Let us now discuss the challenge posed by quantum adversaries. Our aim is to show that, similarly as in the classical case, the extracted bits $\mathsf{E}(X, Y)$ are secure even if the adversary is given Y. Such an adversary prepares a quantum state ρ_x on $\mathcal{Q}$ that depends on $X = x$. To obtain maximal information about $\mathsf{E}(X, Y)$, he performs a measurement on his quantum system Q which depends

on Y. As a result, his (classical) information E is no longer independent of Y. This means that we cannot view this as merely a reduction of the entropy of the source X. Thus we cannot directly prove a statement like Lemma 1 when E is replaced by a quantum system Q. In particular, due to the effect of locking [24], we know that there exist short classical keys (Y) that can unlock a lot of classical information (about X) stored in a quantum system Q. In the first part of this paper we will show that if the extractor E extracts a single bit, we can preclude such locking effect (Theorem III.1).

Before embarking on this analysis, we point out the following straightforward result. If the adversary's measurement does not depend on Y we can essentially apply the classical security proofs. That is, the adversary's measurement produces some classical information E which can be viewed as reducing the entropy of the source X. If the size of the quantum system is sufficiently small, then the random variable E does not give much information about X and therefore the extracted bits look random even to such an adversary. These statements are expressed in the following two lemmas.

Note that we can generalize the guessing-entropy of X given Q to the case where Q is a quantum system. Let $\rho_{XQ} := \sum_{x \in \mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \rho_x$ be a cq-state. Then

$$H_{\mathsf{g}}(X \leftarrow Q) := -\log \max_{\mathcal{E}} \sum_{x \in \mathcal{X}} P_X(x)\mathsf{tr}(E_x\rho_x) , \quad (5)$$

where the maximum is taken over all POVMs $\mathcal{E} := \{E_x\}_{x \in \mathcal{X}}$ on $\mathcal{Q}$.

We now state the non-adaptive quantum version of Proposition 1. It is a direct consequence of the reasoning above.

Proposition 1′. Let $\mathsf{E} : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ be a strong (k, ε)-extractor, and let $\mathcal{F}$ be a POVM on $\mathcal{Q}$. Then for all cq-states ρ_{XQ} with

$$H_{\mathsf{g}}(X \leftarrow Q) \geq k + \log 1/\varepsilon ,$$

we have

$$d(\mathsf{E}(X, Y) \leftarrow Y\mathcal{F}(Q)) \leq 2\varepsilon .$$

The following is the quantum analogue of Lemma 1 (its proof can again be found in Appendix B). It states that a short additional piece of classical information W does not help much in guessing X if the quantum system Q depends only on X. Again, additional independent information V does not help either.

Lemma 1′. Consider a cccq-state ρ_{XVWQ} with $\rho_{XV} = \rho_X \otimes \rho_V$ and $VW \leftrightarrow X \leftrightarrow Q$. Then

$$H_{\mathsf{g}}(X \leftarrow VWQ) \geq H_{\mathsf{g}}(X \leftarrow Q) - H_0(W)$$

and with probability at least $1 - \varepsilon$ over $(v, w) \leftarrow P_{VW}$, we

have

$$H_{\mathsf{g}}(X \leftarrow Q|V = v, W = w) \geq H_{\mathsf{g}}(X \leftarrow Q) - H_0(W) - \log 1/\varepsilon .$$

We now state more precisely what we are aiming to prove about strong extractors. Note that Lemma 1′ only gives a weak security guarantee for the extracted bits $\mathsf{E}(X, Y)$ – they are only shown to be secure against an adversary who measures his quantum state *before* receiving Y. To discuss the stronger type of security we aim for, we first state the definition of the non-uniformity in the quantum case.

Definition 3. Let ρ_{ZQ} be an arbitrary cq-state on $\mathcal{Z} \otimes \mathcal{Q}$. The non-uniformity $d(Z \leftarrow Q)$ of Z given Q is defined as

$$d(Z \leftarrow Q) := \|\rho_{ZQ} - \rho_{\mathcal{U}_{\mathcal{Z}}} \otimes \rho_Q\| ,$$

where $\rho_{\mathcal{U}_{\mathcal{Z}}}$ denotes the completely mixed state on $\mathcal{Z}$.

We describe a few basic properties of this definition in Appendix A. In a cryptographic setting, the condition $d(Z \leftarrow Q) \leq \varepsilon$ for some small ε means that the key Z is secure in a setting where Q is controlled by the adversary; as explained in [15] (see also [16, 22]), such a key is, with probability at least $1 - \varepsilon$, equivalent to a perfectly secure key.

In the sequel, we aim to show that $d(\mathsf{E}(X, Y) \leftarrow YQ)$ is small for certain strong extractors E and appropriate parameters. This means that the extracted bits are secure even if the adversary is given Y in addition to his quantum system.

In the next section, we will show that for extractors with binary output, the quantity of interest can in fact be bounded by considering an adversary whose strategy does not depend on Y, i.e., he performs a measurement independent of Y as in Lemma 1′. We then use this result in Section IV to construct strong extractors that output several bits.

III. EXTRACTORS WITH BINARY OUTPUT

We will first sketch the arguments in this section. For an extractor $\mathsf{e} : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$ with binary output the non-uniformity of the extracted bit $Z = \mathsf{e}(X, Y)$ given Y and the quantum system Q can be directly related to the success probability in distinguishing two quantum states ρ_0^y and ρ_1^y, for each $y \in \mathcal{Y}$. For a given y these are the (generally mixed) states of the adversary, conditioned on the extracted bit being 0 or 1, respectively. We modify an argument by Barnum and Knill [25] to bound the optimal success probability in distinguishing ρ_0^y from ρ_1^y for a given y in terms of the success probability resulting from the use of a pretty good measurement [26] $\mathcal{E}_{pgm}^y$. On the other hand, we will show that there exists a POVM $\mathcal{F}$ which refines all the pretty good measurements $\{\mathcal{E}_{pgm}^y\}_{y \in \mathcal{Y}}$ simultaneously; i.e., the outcome of the measurement $\mathcal{E}_{pgm}^y$ can be obtained by applying $\mathcal{F}$ and

classical post-processing. This POVM $\mathcal{F}$ is a pretty good measurement defined by the states $\{\rho_x\}_{x \in \mathcal{X}}$, the conditional states of Q given $X = x$, or, in the bounded storage model, the states that the adversary prepares upon seeing X. Since the refined measurement $\mathcal{F}$ does not depend on y, we know that it cannot be superior to any classical strategy, see Proposition $1'$, and we obtain the main result of this section, Theorem III.1.

In the next lemma we bound the non-uniformity $d(Z \leftarrow Q)$ of a cq-state $\rho_{ZQ} := \sum_{z \in \{0,1\}} p_z |z\rangle\langle z| \otimes \rho_z$ with binary classical part using a pretty good measurement.

Lemma 2. *Let $\rho_{ZQ} := \sum_{z \in \{0,1\}} p_z |z\rangle\langle z| \otimes \rho_z$ be a cq-state with binary classical part. Then*

$$d(Z \leftarrow Q) \leq \sqrt{2d(Z \leftarrow \mathcal{E}_{pgm}(Q))} + d(Z) , \qquad (6)$$

where $\mathcal{E}_{pgm}$ is the pretty good measurement defined by ρ_{ZQ}, i.e. the POVM elements of this measurement are $E_z := p_z \rho_Q^{-1/2} \rho_z \rho_Q^{-1/2}$ for $z \in \{0,1\}$.

Proof. By definition

$$d(Z \leftarrow Q) = \sum_{z=0}^1 \|p_z \rho_z - \frac{1}{2}\rho_Q\| = \|p_0\rho_0 - p_1\rho_1\|, \quad (7)$$

Let $\Delta := p_0\rho_0 - p_1\rho_1$ and let $\Delta =: A^+ - A^-$ with $A^+ \geq 0$, $A^- \geq 0$ be the decomposition of Δ into a nonnegative and a negative part. Then

$$\|p_0\rho_0 - p_1\rho_1\| = \frac{1}{2}(\text{tr}(A^+) + \text{tr}(A^-))$$
$$= \text{tr}(A^+) - \frac{1}{2}\text{tr}(\Delta)$$
$$= \text{tr}(\mathbb{P}\Delta) - \frac{1}{2}(p_0 - p_1),$$

where $\mathbb{P}$ is the projector onto the support of A^+. We will do some work to show that

$$\text{tr}(\mathbb{P}\Delta) \leq \sqrt{2d(Z \leftarrow \mathcal{E}_{pgm}(Q))} , \qquad (8)$$

where $\mathcal{E}_{pgm}$ is the pretty good measurement that distinguishes ρ_1 and ρ_1. By noting that

$$-\frac{1}{2}(p_0 - p_1) \leq \frac{1}{2}|p_0 - p_1| \leq \frac{1}{2}\left(|p_0 - \frac{1}{2}| + |p_1 - \frac{1}{2}|\right)$$
$$= d(Z) ,$$

we obtain the desired result, Eq. (6). Consider thus the quantity $\text{tr}(\mathbb{P}\Delta)$. We can bound

$$\text{tr}(\mathbb{P}\Delta) \leq \sqrt{\text{tr}(A^\dagger A)\text{tr}(B^\dagger B)} \qquad (9)$$

by applying the operator Cauchy-Schwarz inequality to

the operators

$$A := \rho_Q^{1/4}\mathbb{P}\rho_Q^{1/4}$$
$$B := \rho_Q^{-1/4}\Delta\rho_Q^{-1/4}.$$

But

$$\text{tr}(A^\dagger A) = \text{tr}(\rho_Q^{1/2}\mathbb{P}\rho_Q^{1/2}\mathbb{P})$$
$$\leq \text{tr}(\rho_Q^{1/2}\mathbb{P}\rho_Q^{1/2})$$
$$\leq \text{tr}(\rho_Q) = 1 \qquad (10)$$

where we used the fact that $\mathbb{P} \leq 1$ and the fact that $\rho_Q^{1/2}\mathbb{P}\rho_Q^{1/2}$ is nonnegative. On the other hand, by the definition of the pretty good measurement $\mathcal{E}_{pgm} = \{E_0, E_1\}$ we have

$$\text{tr}(B^\dagger B) = \text{tr}(\rho_Q^{-1/2}\Delta\rho_Q^{-1/2}\Delta)$$
$$= \text{tr}(E_0\Delta) - \text{tr}(E_1\Delta)$$
$$= P_{succ}(\mathcal{E}_{pgm}) - p_1\text{tr}(E_0\rho_1) - p_0\text{tr}(E_1\rho_0)$$
$$= 2P_{succ}(\mathcal{E}_{pgm}) - 1 . \qquad (11)$$

Here we have used the definition of the success probability $P_{succ}(\{E_0, E_1\}) := p_0\text{tr}(E_0\rho_0) + p_1\text{tr}(E_1\rho_1)$, and the fact that $E_0 + E_1 = 1$ and $p_0 + p_1 = 1$ in the last step. Note that probability of success $P_{succ}(\mathcal{E})$ for a fixed POVM $\mathcal{E}$ is the same as the probability of successfully distinguishing an instance drawn from the distribution $\mathcal{E}(\rho_0)$ and $\mathcal{E}(\rho_1)$, respectively, with a priori probabilities p_0 and p_1. Now we invoke Helstrom's theorem [27] which says that the success probability of distinguishing two quantum states σ_0 and σ_1 with priors p_0 and p_1 using an optimal POVM $\mathcal{E}_{opt}$ is equal to $P_{succ}(\mathcal{E}_{opt}) = \frac{1}{2} + \|p_0\sigma_0 - p_1\sigma_1\|$. We apply this theorem for $\sigma_z = \mathcal{E}_{pgm}(\rho_z)$ and write $P_{succ}(\mathcal{E}_{pgm}) = \frac{1}{2} + d(Z \leftarrow \mathcal{E}_{pgm}(Q))$ (cf. Eq. (7)). Combining this with Eqs. (9), (10) and (11) yields Eq. (8), as desired. $\qquad \square$

Now the goal is to bound the non-uniformity $d(\mathsf{e}(X,Y) \leftarrow YQ)$ for extractors e with binary output when Q is a quantum system which depends on X. For this we consider the cccq-state $\rho_{ZXYQ} \equiv \rho_{\mathsf{e}(X,Y)XYQ}$ which has the form

$$\rho_{ZXYQ} = \sum_{y,x,z=\mathsf{e}(x,y)} P_X(x)P_Y(y)|xyz\rangle\langle xyz| \otimes \rho_x ,$$
$$(12)$$

where $P_Y(y) = \frac{1}{|\mathcal{Y}|}$ for every $y \in \mathcal{Y}$. For this state one can express the non-uniformity $d(Z \leftarrow YQ)$ as (cf. Eq. (2))

$$\mathbb{E}_{y \leftarrow P_Y}\Big[\sum_{z \in \{0,1\}} \|\sum_x P_{Z|X=x,Y=y}(z)P_X(x)\rho_x - \frac{1}{2}\rho_Q\|\Big] .$$
$$(13)$$

Note that $P_{Z|X=x,Y=y}(z)$ is 1 or 0, depending on whether

or not $\mathsf{e}(x, y) = z$. It is straightforward to verify that

$$p_z^y \rho_z^y := \sum_{x \in \mathcal{X}} P_{Z|Y=y}(z) P_{X|Y=y,Z=z}(x) \rho_x$$

$$= \sum_{x \in \mathcal{X}} P_{Z|X=x,Y=y}(z) P_X(x) \rho_x \; , \qquad (14)$$

where we introduced for each $y \in \mathcal{Y}$ and $z \in \{0, 1\}$ the density matrix

$$\rho_z^y := \sum_{x \in \mathcal{X}} P_{X|Y=y,Z=z}(x) \rho_x \; , \qquad (15)$$

with the normalising factor

$$p_z^y := P_{Z|Y=y}(z) = \Pr_{x \leftarrow X} [\mathsf{e}(x, y) = z] \; . \qquad (16)$$

The state ρ_z^y is the state of Q conditioned on $\mathsf{e}(X, y) = z$; for any given $y \in \mathcal{Y}$, the two states ρ_0^y and ρ_1^y have a priori probabilities p_z^y with $z \in \{0, 1\}$. From this definition, it is clear that

$$\sum_z p_z^y \rho_z^y = \rho_Q \; , \qquad (17)$$

which is *independent* of y. This observation will be essential in the proof of the following theorem.

Applying Helstrom's theorem gives an intuitive interpretation of the quantity of interest (which we state, but do not need later in the proof): $\frac{1}{2} + d(\mathsf{e}(X, Y) \leftarrow YQ)$ is the maximal average success probability when distinguishing ρ_0^y and ρ_1^y with a priori probabilities p_0^y and p_1^y, over random $y \leftarrow P_Y$. This follows by combining Eq. (17) with Eq. (13) and Eqs. (15), (16).

We are ready to derive the main result of this section:

Theorem III.1. *Let* $\mathsf{e} : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$ *be a strong* (k, ε)-*extractor. Then for all* ρ_{XQ} *with*

$$H_{\mathsf{g}}(X \leftarrow Q) \geq k + \log 1/\varepsilon \; ,$$

we have

$$d(\mathsf{e}(X, Y) \leftarrow YQ) \leq 3\sqrt{\varepsilon} \; ,$$

where $\rho_{YXQ} := \rho_{\mathcal{U}_{\mathcal{Y}}} \otimes \rho_{XQ}$.

Proof. By Eq. (2) (cf. Eq. (A3)) we can express

$$d(\mathsf{e}(X, Y) \leftarrow YQ) = \mathop{\mathbb{E}}_{y \leftarrow P_Y} [d(\mathsf{e}(X, y) \leftarrow Q)] \; . \qquad (18)$$

We can apply the pretty good measurement bound of Lemma 2 for each $y \in \mathcal{Y}$ to the state $\rho_{\mathsf{e}(X,y)Q} = \sum_{z \in \{0,1\}} p_z^y |z\rangle\langle z| \otimes \rho_z^y$, where the density matrices ρ_z^y and their associated probabilities p_z^y are defined in Eqs. (15) and (16). We get

$$d(\mathsf{e}(X, y) \leftarrow Q) \leq \sqrt{2d(\mathsf{e}(X, y) \leftarrow \mathcal{E}_{pgm}^y(Q))} + d(\mathsf{e}(X, y))$$

for every $y \in \mathcal{Y}$. Taking the expectation over $y \leftarrow P_Y$ again and using the convexity of the square root gives

$$d(\mathsf{e}(X, Y) \leftarrow YQ) \leq \sqrt{\mathop{\mathbb{E}}_{y \leftarrow P_Y} [2d(\mathsf{e}(X, y) \leftarrow \mathcal{E}_{pgm}^y(Q))]} + d(\mathsf{e}(X, Y) \leftarrow Y) \qquad (19)$$

by Eq. (2) (see also Eq. (A2)). Since

$$H_\infty(X) \geq H_{\mathsf{g}}(X \leftarrow Q) \; ,$$

the second term in Eq. (19) is upper bounded by ε. Let us now consider the details of the pretty good measurement $\mathcal{E}_{pgm}^y$. The measurement $\mathcal{E}_{pgm}^y = \{E_z^y\}_{z \in \{0,1\}}$ is determined by the POVM elements

$$E_z^y := p_z^y (G^y)^{-1/2} \rho_z^y (G^y)^{-1/2} \qquad (20)$$

where, as argued above (Eq. (17)),

$$G^y = \sum_{z \in \mathcal{Z}} p_z^y \rho_z^y = \rho_Q \; . \qquad (21)$$

is independent of y. This fact allows us to define a new pretty good measurement $\mathcal{F}$ which does not depend on y, but is equally good or better in estimating Z from Q and Y. This new pretty good measurement $\mathcal{F} = \{F_x\}_{x \in \mathcal{X}}$ has POVM elements

$$F_x := P_X(x) \rho_Q^{-1/2} \rho_x \rho_Q^{-1/2} \; .$$

Expressed differently, $\mathcal{F}$ is simply the pretty good measurement defined by the ensemble $\{P_X(x), \rho_x\}$. From Eqs. (14), (20) and (21) above one can see that

$$E_z^y = \sum_{x \in \mathcal{X}} P_{Z|X=x,Y=y}(z) F_x \qquad (22)$$

In other words, the results of the measurements $\{\mathcal{E}_{pgm}^y\}_{y \in \mathcal{Y}}$ can in fact be obtained by first estimating x by measuring the quantum system Q with $\mathcal{F} = \{F_x\}_{x \in \mathcal{X}}$. Then we infer z for a given y by computing $z = \mathsf{e}(x, y)$. On a more technical level, one needs to show that for every $y \in \mathcal{Y}$ the non-uniformity given the measurement outcome of the measurement $\mathcal{E}_{pgm}^y$ is smaller than or equal to the non-uniformity given the outcome of the refined measurement $\mathcal{F}$. We have summarized these technical details in Lemma 6 proved in Appendix C. Formally, we have

$$d(\mathsf{e}(X, y) \leftarrow \mathcal{E}_{pgm}^y(Q)) \leq d(\mathsf{e}(X, y) \leftarrow \mathcal{F}(Q)) \; .$$

Taking the expectation over $y \leftarrow P_Y$ gives (cf. Eq. (A3))

$$\mathop{\mathbb{E}}_{y \leftarrow P_Y} [d(\mathsf{e}(X, y) \leftarrow \mathcal{E}_{pgm}^y(Q))] \leq d(\mathsf{e}(X, Y) \leftarrow Y\mathcal{F}(Q)) \; .$$

Since $\mathcal{F}$ does not depend on y we have reduced our problem to the simple scenario where the quantum system is measured before the adversary obtains y. Thus we can

apply Proposition 1′,

$$d(\mathsf{e}(X,Y) \leftarrow Y\mathcal{F}(Q)) \leq 2\varepsilon . \qquad (23)$$

We conclude with Eq. (19) that

$$d(\mathsf{e}(X,Y) \leftarrow YQ) \leq 2\sqrt{\varepsilon} + \varepsilon ,$$

hence the claim follows. $\qquad\square$

We now show that even if the adversary is given additional information V which is independent of X and a short bit string W which might depend on X, the extracted bit looks secure. This statement will be used below to prove that certain extractors which output several bits can also safely be used in a cryptographic context (cf. Theorem IV.1).

Corollary III.2. *Let* $\mathsf{e} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ *be a strong* (k,ε)-*extractor. Let* ρ_{XVWQ} *be a cccq-state with* $\rho_{XV} = \rho_X \otimes \rho_V$, $VW \leftrightarrow X \leftrightarrow Q$ *and*

$$H_{\mathsf{g}}(X \leftarrow Q) \geq k + H_0(W) + 2\log 1/\varepsilon .$$

Then

$$d(\mathsf{e}(X,Y) \leftarrow YVWQ) \leq 4\sqrt{\varepsilon} ,$$

where $\rho_{YXVWQ} := \rho_{\mathcal{U}_{\mathcal{Y}}} \otimes \rho_{XVWQ}$.

Proof. Let $\alpha := d(\mathsf{e}(X,Y) \leftarrow YVWQ)$ be the quantity of interest. Then by Eq. (2) (see also Eq. (A2)),

$$\alpha = \mathop{\mathbb{E}}_{(v,w)\leftarrow P_{VW}} \left[d(\mathsf{e}(X,Y) \leftarrow YQ | V=v, W=w) \right] ,$$

where the term in brackets is the non-uniformity of $\mathsf{e}(X,Y)$ with respect to the conditional state $\rho_{XQ|V=v,W=w}$. By Lemma 1′, we have

$$H_{\mathsf{g}}(X \leftarrow Q | V=v, W=w) \geq k + \log 1/\varepsilon \qquad (24)$$

with probability at least $1-\varepsilon$ over random $(v,w) \leftarrow P_{VW}$. For any (v,w) for which Eq. (24) is satisfied, we have

$$d(\mathsf{e}(X,Y) \leftarrow YQ | V=v, W=w) \leq 3\sqrt{\varepsilon}$$

by Theorem III.1. Thus

$$\alpha \leq 3\sqrt{\varepsilon} + \varepsilon ,$$

and the claim follows. $\qquad\square$

IV. EXTRACTORS WITH NONBINARY OUTPUT

In this section we will consider strong extractors which output several bits. We first show how to use independent seeds $y_1, \ldots, y_m$ to extract m bits. The security of the extracted bits in the quantum setting will follow from applying our bound for binary extractors, Theorem III.1

in combination with a quantum version of the so-called hybrid argument. By a similar technique, we will show how to extract more bits under stronger assumptions. Let us first discuss the hybrid argument.

Consider a cq-state of the form ρ_{ZQ}, where $Z = (Z_1, \ldots, Z_m)$ is an m-bit string. We aim to find a bound on $d(Z \leftarrow Q)$ in terms of non-uniformities of binary random variables.

By definition, we have

$$d(Z \leftarrow Q) = \| \rho_{ZQ} - \rho_{\mathcal{U}_{\{0,1\}}}^{\otimes m} \otimes \rho_Q \| .$$

Let us define for $i = 0, \ldots, m$ the states

$$\rho^{(i)} := \rho_{\mathcal{U}_{\{0,1\}}}^{\otimes m-i} \otimes \rho_{Z^i Q}$$

on $\{0,1\}^m \otimes \mathcal{Q}$, where we use the abbreviation $z^i := (z_1, \ldots, z_i)$ to refer to the first i bits of $z \in \{0,1\}^m$. Clearly, we have $\rho^{(m)} = \rho_{ZQ}$ and $\rho^{(0)} = \rho_{\mathcal{U}_{\{0,1\}}}^{\otimes m} \otimes \rho_Q$. We use the "telescoping" sum

$$\rho^{(0)} - \rho^{(m)} = \sum_{i=0}^{m-1} \rho^{(i)} - \rho^{(i+1)} ,$$

which by the triangle inequality implies that

$$d(Z \leftarrow Q) \leq \sum_{i=0}^{m-1} \| \rho^{(i+1)} - \rho^{(i)} \| .$$

But

$$\begin{aligned}
\| \rho^{(i+1)} - \rho^{(i)} \| &= \| \rho_{\mathcal{U}_{\{0,1\}}}^{\otimes m-i-1} \otimes \rho_{Z^{i+1}Q} - \rho_{\mathcal{U}_{\{0,1\}}}^{\otimes m-i} \otimes \rho_{Z^i Q} \| \\
&= \| \rho_{Z^{i+1}Q} - \rho_{\mathcal{U}_{\{0,1\}}} \otimes \rho_{Z^i Q} \| \\
&= \| \rho_{Z_{i+1}Z^i Q} - \rho_{\mathcal{U}_{\{0,1\}}} \otimes \rho_{Z^i Q} \|
\end{aligned}$$

We thus arrive at the following conclusion

$$d(Z \leftarrow Q) \leq \sum_{i=0}^{m-1} d(Z_{i+1} \leftarrow Z^i Q) . \qquad (25)$$

Let us now state and prove the main theorem.

Theorem IV.1. *Let* $\mathsf{e} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ *be a strong* (k,ε)-*extractor, and let*

$$\begin{aligned}
\mathsf{E}^m &: \mathcal{X} \times \mathcal{Y}^m \to \{0,1\}^m \\
(x, y_1, \ldots, y_m) &\mapsto (\mathsf{e}(x,y_1), \ldots, \mathsf{e}(x,y_m)) .
\end{aligned}$$

Then for all cq-states ρ_{XQ} with

$$H_{\mathsf{g}}(X \leftarrow Q) \geq k + m + 2\log 1/\varepsilon , \qquad (26)$$

we have

$$d(\mathsf{E}^m(X,Y^m) \leftarrow Y^m Q) \leq 4m\sqrt{\varepsilon} ,$$

where $\rho_{Y^m XQ} := \rho_{\mathcal{U}_{\mathcal{Y}^m}} \otimes \rho_{XQ}$.

Proof. We use Eq. (25) to get

$$d(\mathsf{E}^m(X, Y^m) \leftarrow Y^m Q) \leq \sum_{i=0}^{m-1} d(Z_{i+1} \leftarrow Z^i Y^m Q) \ , \tag{27}$$

where $Z^m \equiv \mathsf{E}^m(X, Y^m)$. Observe that $(Y_{i+2}, \ldots, Y_m)$ is independent of $Z^{i+1} Y^{i+1} Q$, which by Eq. (A4) gives

$$d(Z_{i+1} \leftarrow Z^i Y^m Q) = d(Z_{i+1} \leftarrow Z^i Y^{i+1} Q) \ . \tag{28}$$

But

$$\begin{aligned} d(Z_{i+1} \leftarrow Z^i Y^{i+1} Q) &= d(Z_{i+1} \leftarrow Y_{i+1} Z^i Y^i Q) \\ &= d(\mathsf{e}(X, \tilde{Y}) \leftarrow \tilde{Y} \mathsf{E}^i(X, Y^i) Y^i Q) \end{aligned}$$

where $\tilde{Y} \equiv Y_{i+1}$. Applying Corollary III.2 to $(V, W) = (Y^i, \mathsf{E}^i(X, Y^i))$ yields

$$d(Z_{i+1} \leftarrow Z^i Y^{i+1} Q) \leq 4\sqrt{\varepsilon} \tag{29}$$

for every $i = 0, \ldots, m-1$. We have made use of the fact that $H_0(W) = H_0(\mathsf{E}^i(X, Y^i)) \leq m$ by definition. The claim then follows from Eqs. (27), (28) and (29). $\qquad\square$

In the next section, we study the implications of Theorem IV.1 for the bounded storage model. We will see that the bound on the storage of the adversary translates into an upper bound on the guessing probability, as required (cf. Eq. (26)). We will then give a concrete example of an extractor for the bounded storage model with quantum adversaries.

Before continuing, however, let us point out that in certain situations, we can use the hybrid argument to show that the seed Y can be reused several times. This gives more efficient randomness extractors (under stronger assumptions about the inital cq-state ρ_{XQ}). Following similar terminology in the literature on extractors, we introduce the following notion.

Definition 4. *A cq-state ρ_{XQ} where $X = (X_1, \ldots, X_m)$ consists of m parts is a k-blockwise state if for all $i = 0, \ldots, m-1$*

$$H_{\mathsf{g}}(X_{i+1} \leftarrow X^i Q) \geq k \ .$$

We will now show how to extract multiple bits from such a cq-state by reusing the seed. This is interesting for several reasons. First, k-blockwise states arise naturally in realistic situations such as the bounded storage model. We will discuss this in more detail below (cf. Section V C). Second, extractors for k-blockwise probability distributions are often used to construct (classical) extractors by transforming the input distribution to a k-blockwise distribution. It might therefore be possible to obtain extractor constructions for the quantum case using similar lines of reasoning.

Theorem IV.2. *Let $\mathsf{e} : \mathcal{X} \times \mathcal{Y} \rightarrow \{0,1\}$ be a strong (k, ε)-extractor, and let*

$$\begin{aligned} \tilde{\mathsf{E}}^L &: \mathcal{X}^L \times \mathcal{Y}^m \rightarrow \{0,1\}^{Lm} \\ (x_1, \ldots, x_L, y) &\mapsto (\mathsf{E}^m(x_1, y), \ldots, \mathsf{E}^m(x_L, y)) \ , \end{aligned}$$

where $\mathsf{E}^m : \mathcal{X} \times \mathcal{Y}^m \rightarrow \{0,1\}^m$ is defined as in Theorem IV.1. Then

$$d(\tilde{\mathsf{E}}^L(X^L, Y) \leftarrow YQ) \leq 4Lm\sqrt{\varepsilon} \ ,$$

for all $(k+m+2\log 1/\varepsilon)$-blockwise states ρ_{XQ} on $\mathcal{X}^L \otimes \mathcal{Q}$, where $\rho_{YXQ} := \rho_{\mathcal{U}_{\mathcal{Y}}} \otimes \rho_{XQ}$.

Proof. With Eq. (25) we get

$$d(\tilde{\mathsf{E}}^L(X^L, Y) \leftarrow YQ) \leq \sum_{i=0}^{L-1} d(Z_{i+1} \leftarrow Z^i YQ) \ , \tag{30}$$

where $Z^L \equiv \tilde{\mathsf{E}}^L(X^L, Y)$. Since (Z^i, Y) is a function of (X^i, Y) and since applying functions does not increase the trace distance, we obtain

$$d(\tilde{\mathsf{E}}^L(X^L, Y) \leftarrow YQ) \leq \sum_{i=0}^{L-1} d(Z_{i+1} \leftarrow X^i YQ) \ . \tag{31}$$

But $d(Z_{i+1} \leftarrow X^i YQ) = d(\mathsf{E}^m(X_{i+1}, Y) \leftarrow YX^i Q)$, and $\rho_{YX_{i+1}X^i Q} = \rho_{\mathcal{U}_{\mathcal{Y}}} \otimes \rho_{X_{i+1}X^i Q}$. Moreover,

$$H_{\mathsf{g}}(X_{i+1} \leftarrow X^i Q) \geq k + m + 2\log 1/\varepsilon \ .$$

by assumption. Thus we can apply Theorem IV.1 and the claim follows. $\qquad\square$

V. THE BOUNDED STORAGE MODEL WITH A QUANTUM ADVERSARY

A. Bounded storage, guessing entropy and extractors

In the classical version of the bounded storage model, the security of the extracted bits is a direct consequence of the property of the extractor given in Proposition 1 and the fact that an adversary has limited information about X. The latter fact is expressed by the following well-known proposition, whose proof we omit, as it is trivial. It states that an adversary who has $H_0(E)$ bits of storage can not predict X well.

Proposition 2. *Let P_{XE} be an arbitrary distribution. Then*

$$H_{\mathsf{g}}(X \leftarrow E) \geq H_{\infty}(X) - H_0(E) \ .$$

Together with Lemma 1, it follows that a strong (k, ϵ)-extractor has the property that $d(\mathsf{e}(X, Y) \leftarrow YE) \leq 2\epsilon$

for all P_{XE} with

$$H_\infty(X) \geq k + H_0(E) + \log 1/\varepsilon .$$

Thus the security of the extracted key can be directly derived from the strong extractor property and the bounded-storage assumption. The main challenge is to construct strong extractors which satisfy all the additional requirements for applicability in the bounded storage model (see Section V B).

What about quantum storage? We show that a similar reasoning applies; given an extractor which is characterized by the guessing-entropy $H_g(X \leftarrow Q)$, the storage bound can be translated into a security guarantee. We first show that X can not be guessed by measuring Q when the number of qubits constituting Q is limited.

Proposition 2′. *Let ρ_{XQ} be a cq-state. Then*

$$H_g(X \leftarrow Q) \geq H_\infty(X) - H_0(Q) .$$

Proof. Consider a POVM $\mathcal{E} := \{E_x\}_{x \in \mathcal{X}}$ on $\mathcal{Q}$ that maximizes the expression defining $H_g(X \leftarrow Q)$ (cf. Eq (5)). Then

$$2^{-H_g(X \leftarrow Q)} = \sum_x P_X(x)\mathsf{tr}(E_x \rho_x)$$
$$= \mathsf{tr}\Big(\big(\sum_x |x\rangle\langle x| \otimes E_x\big)\rho_{XQ}\Big)$$
$$\leq 2^{-H_\infty(XQ)}\mathsf{tr}\Big(\sum_x |x\rangle\langle x| \otimes E_x\Big) .$$

The statement then follows from the fact that

$$\mathsf{tr}\Big(\sum_x |x\rangle\langle x| \otimes E_x\Big) = \mathsf{tr}\Big(\sum_x E_x\Big) = \mathsf{tr}(1_\mathcal{Q}) = 2^{H_0(Q)} .$$

$\square$

By combining Proposition 2′ with Theorem IV.1, we obtain a way of constructing strong extractors for the bounded storage model in the presence of quantum adversaries: the statement of Theorem IV.1 holds when Eq. (26) is replaced by the weaker condition

$$H_\infty(X) \geq k + m + H_0(Q) + 2\log 1/\varepsilon . \tag{32}$$

Before applying this result to obtain a concrete construction, let us elaborate on a recent example which shows that not every strong extractor yields secure bits in the quantum bounded storage model.

Remark V.1. *Gavinsky, Kempe and de Wolf [20] consider the function*

$$\mathsf{e} : \{0,1\}^n \times \omega_n \qquad \rightarrow \qquad \{0,1\}$$
$$((x_1, \ldots, x_n), \{y_1, y_2\}) \qquad \mapsto \qquad x_{y_1} \oplus x_{y_2} ,$$

where $\oplus$ denotes bitwise addition modulo 2 and where ω_n is the set of pairs (y_1, y_2) of distinct indices $y_1, y_2 \in$

$\{1, \ldots, n\}$. *They then study the function E^m restricted to the set $\{0,1\}^n \times \Omega_m$, where $\Omega_m \subset \omega_n^m$ is the subset of disjoint m-tuples. Let us call this restriction $\tilde{\mathsf{E}}_m$ and let $\tilde{Y}_m$ be uniform on Ω_m. In our terminology, they show the following. There is an $\alpha \approx 1/\sqrt{\log n}$ such that for large enough n and $m := \alpha n$, the quantity $d(\tilde{\mathsf{E}}_m(X, \tilde{Y}_m) \leftarrow \tilde{Y}_m E)$ is small for any classical random variable E with $H_0(E) \leq \sqrt{n}$, whereas $d(\tilde{\mathsf{E}}_m(X, \tilde{Y}_m) \leftarrow \tilde{Y}_m Q)$ is large if Q is quantum and $H_0(Q)$ is polylogarithmic in n.*

This statement does not contradict Theorem IV.1 which can not be applied in this situation. This is because the function $\tilde{E}_m$ does not have the required form. While Theorem III.1 tells us that the difference between classical and quantum prior information is limited in the case of extractors with binary output, this example shows that the case of general extractors which output several bits is more subtle.

B. Extractors for the bounded storage model: an explicit example

In this section, we give a concrete example of a function $\mathsf{E} : \{0,1\}^n \times \{0,1\}^t \rightarrow \{0,1\}^m$ which can be used in the bounded storage model in the presence of a quantum adversary. Let us first discuss what additional requirements such a function has to satisfy.

Typical parameters of the bounded storage model are as follows: For some $1 \geq \alpha > \beta > 0$, $H_\infty(X) \geq \alpha n$ and $H_0(Q) \leq \beta n$. Here, the parameter α is called the *min-entropy rate*, whereas β is referred to as the *storage rate*. The amount of memory available to the honest parties, Alice and Bob, on the other hand, is supposed to be much more limited. Typically, it is assumed that they have only $O(\log n)$ bits of storage. Expressed differently, the scheme should be secure even if the adversary is significantly more powerful than the participating honest parties.

The fact that Alice and Bob have only $O(\log n)$ bits of memory implies that the strong extractor must have seed length $\log |\mathcal{Y}| = t$ of that order. Moreover, the extractor has to be (efficiently) computable with limited memory. This is the case if E is ℓ-local, meaning that it only depends on a small number ℓ (instead of n) physical bits of its first argument, where the ℓ bit locations are determined by the second argument. Note that a different solution to the latter problem was suggested by Lu [11], who considers so-called on-line computable functions.

Due to these requirements, finding explicit, efficiently computable constructions for the bounded-storage model is a rather intricate problem, which has been studied for some time [8, 9, 10, 11, 12]. Here we consider a construction by Vadhan. By choosing the output to be a single bit, Theorem 8.5 in [12] gives an ℓ-local strong

(k, ε)-extractor $\mathsf{e} : \{0, 1\}^n \times \{0, 1\}^t \to \{0, 1\}$ with

$$t = \log n + O(\log 1/\varepsilon) \qquad (33)$$

$$\ell = \frac{3}{2} \frac{n}{k} + O(\log 1/\varepsilon) \qquad (34)$$

for every $\varepsilon > \exp(-n/2^{O(\log^* n)})$.

Suppose we want to achieve an error ε, using Theorem IV.1. Then the error for the one-bit-extractor e must be upper bounded by $(\varepsilon/4m)^2$. Inserting this into Eqs. (33) and (34) gives

Corollary V.2. *For any $\varepsilon > 4m \exp(-n/2^{O(\log^* n)})$, there is an ℓ-local function*

$$\mathsf{E} : \{0, 1\}^n \times \{0, 1\}^t \to \{0, 1\}^m ,$$

with

$$t = m \log n + O(m \log m + m \log 1/\varepsilon)$$

$$\ell = \frac{3}{2} \frac{nm}{k - m - 2 \log 1/\varepsilon} + O(m \log m + m \log 1/\varepsilon) ,$$

such that $d(\mathsf{E}(X, Y) \leftarrow YQ) \leq \varepsilon$ for all ρ_{XQ} with

$$H_\infty(X) - H_0(Q) \geq k ,$$

where $\rho_{YXQ} = \rho_{\mathcal{U}_{\{0,1\}^d}} \otimes \rho_{XQ}$.

In terms of the min-entropy rate α and the storage-rate β, our result implies that for any $\alpha > \beta$, there is an extractor which uses $O(m \log n + m \log 1/\varepsilon)$ bits of initial key, outputs m bits with security ε, and reads $O(m \log m + m \log 1/\varepsilon)$ bits from the randomizer X. In comparison, the best known classical construction uses $O(\log n + \log 1/\varepsilon)$ bits of key and reads $O(m + \log 1/\varepsilon)$ from X.

C. Independent randomizers

In the so-called satellite scenario [8], the randomizer X is assumed to consist of a sequence of random bits that are publicly broadcast in sequence. In this situation, it is clear that if we partition X into blocks $X = (X_1, \dots, X_L)$, the random variables corresponding to the blocks are independent. What is more interesting is that if the adversary is allowed to prepare a quantum system Q adaptively, the resulting cq-state ρ_{XQ} is a k-blockwise state. This is a consequence of the fact that taking the previous blocks X^i into account when storing and retrieving information about X_{i+1} does not help the adversary if X_{i+1} is independent of X^i. We can express this formally by the following result, with the set $\mathcal{S}$ corresponding to all states on a Hilbert space of limited dimension in the bounded storage model.

Lemma 3. *Let $P_{XX'} = P_X \cdot P_{X'}$ be a probability distribution of independent random variables and let $\mathcal{S}$ be a set of states. Then*

$$\min_{\rho_{XX'Q}} H_\mathsf{g}(X \leftarrow X'Q) \geq \min_{\rho_{XQ}} H_\mathsf{g}(X \leftarrow Q) , \qquad (35)$$

where the minima are over all states of the form

$$\rho_{XX'Q} = \sum_{x,x'} P_{XX'}(x, x') |x\rangle\langle x| \otimes |x'\rangle\langle x'| \otimes \rho_x^{x'}$$

with $\rho_x^{x'} \in \mathcal{S}$ and

$$\rho_{XQ} = \sum_x P_X(x) |x\rangle\langle x| \otimes \rho_x , \qquad \rho_x \in \mathcal{S} ,$$

respectively.

Proof. Let $\{\rho_x^{x'}\}_{x,x'}$ be a family of states such that the corresponding state $\rho_{XX'Q}$ achieves the minimum on the l.h.s. of Eq. (35). Then

$$2^{-H_\mathsf{g}(X \leftarrow X'Q)} = \mathop{\mathbb{E}}_{x' \leftarrow P_{X'}} [2^{-H_\mathsf{g}(X \leftarrow Q | X' = x')}] .$$

But

$$2^{-H_\mathsf{g}(X \leftarrow Q | X' = x')} = \max_{\{E_x\}_x} \sum_{x \in \mathcal{X}} P_X(x) \mathsf{tr}(E_x \rho_x^{x'})$$

$$= 2^{-H_\mathsf{g}(X \leftarrow Q)} ,$$

where the latter expression denotes the guessing entropy of X given Q in the state

$$\rho_{XQ}^{x'} = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle\langle x| \otimes \rho_x^{x'} .$$

The claim directly follows from this. $\qquad \square$

If the randomizer X consists of several independent parts $X = (X_1, \dots, X_L)$ which satisfy $H_\infty(X_i) \geq H_0(Q) + k$ for all i, we can therefore use our hybrid construction (Theorem IV.2) in conjunction with Corollary V.2. As an example, consider the case where each of the blocks X_i consists of n bits with min-entropy rate α. We then obtain an extractor $\mathsf{E} : \{0, 1\}^{Ln} \times \{0, 1\}^t \to \{0, 1\}^{Lm}$ which uses $t = mO(\log n + \log L + \log 1/\varepsilon)$ bits of initial key, reads $mO(\log m + \log L + \log 1/\varepsilon)$ bits from X and gives an ε-secure output in the presence of an adversary with storage rate $\beta < \alpha$. In particular, this construction can extend the key of the honest parties by more than the number of initial key bits. This implies that Alice and Bob end up with a longer key even if the adversary later learns the initial key Y.

VI. TOMOGRAPHY-BASED APPROACH TO GENERAL EXTRACTORS

The results of Section III imply that the security of a single extracted bit is similar with respect to an adversary that has quantum instead of classical resources.

This is not true for general extractors which output several bits, as shown in [20] by an explicit counterexample. It is however possible to give constructions that extract multiple bits in a useful way, as we have shown in the previous section.

Which constructions give rise to "useful" extractors in a quantum context? In this section, we elaborate on this question, showing that general extractors can be used in the setting of privacy amplification, *if* the adversary's memory is limited. Note that the setting of privacy amplification imposes less stringent requirements on the extractor than the setting of the bounded-storage model. Nevertheless, the only construction known to work in the quantum setting has been two-universal hashing [13, 14, 15, 16].

While two-universal hashing has the advantage that it extracts all the randomness present in the source (i.e., the number of extracted bits can be as large as $H_\infty(X) - 2\log 1/\varepsilon$), it requires a long seed Y. Viewed as an extractor, two-universal hashing has the form $\mathsf{E} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$, i.e., the seed is of the same length as the source X. When applied to privacy amplification, this means that n bits need to be communicated from Alice to Bob. We will show below that by considering general extractors the amount of communication can be reduced to approximately the number of qubits the adversary controls. This is important for applications such as the protocols proposed in [18].

We use a measurement-based approach, which bounds the trace distance in terms of the outcomes of a tomographic measurement in mutually unbiased bases. More precisely, we will use the following lemma, whose proof is analogous to a proof in [24].

Lemma 4. *Let A be a hermitian operator on $\mathcal{Q}$, where $d := \dim \mathcal{Q} = p^n$ is a prime power. Then there is POVM $\mathcal{F}$ such that*

$$\|A\| \leq (d+1) \cdot \|\mathcal{F}(A)\| \ .$$

We can then show the following:

Lemma 5. *Let $\mathsf{E} : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a strong (k,ε)-extractor. Then*

$$d(\mathsf{E}(X,Y) \leftarrow YQ) \leq 4 \cdot 2^{H_0(Q)} \cdot \varepsilon \ , \qquad (36)$$

for all cq-states ρ_{XQ} with

$$H_{\mathsf{g}}(X \leftarrow Q) \geq k + \log 1/\varepsilon \ ,$$

and $2^{H_o(Q)} = p^m$ for some prime p.

Remark VI.1. *We point out that the condition on the dimension of Q can easily be dropped by using a different measurement than the one described in Lemma 4, at the cost of introducing an additional constant in the exponent on the r.h.s. of Eq. (36).*

Proof. By definition and Eq. (2),

$$d(\mathsf{E}(X,y) \leftarrow Q) = \sum_{z \in \mathcal{Z}} \|P_{\mathsf{E}(X,y)}(z)\rho_y^z - \frac{1}{|\mathcal{Z}|}\rho_Q\| \ ,$$

where ρ_y^z is the conditional state $\rho_y^z := \rho_{Q|\mathsf{E}(X,y)=z}$ for all $(y,z) \in \mathcal{Y} \times \mathcal{Z}$. By Lemma 4, we get

$$d(\mathsf{E}(X,y) \leftarrow Q)$$
$$\leq 2^{H_o(Q)+1} \sum_{z \in \mathcal{Z}} \|P_{\mathsf{E}(X,y)}(z)\mathcal{F}(\rho_y^z) - \frac{1}{|\mathcal{Z}|}\mathcal{F}(\rho_Q)\| \ ,$$

and thus by taking the expectation over $y \leftarrow P_Y$ with Eq. (2) (see also Eq. (A3))

$$d(\mathsf{E}(X,Y) \leftarrow YQ) \leq 2^{H_o(Q)+1} \, d(\mathsf{E}(X,Y) \leftarrow Y\mathcal{F}(Q)) \ .$$

The claim then follows from Proposition 1′. □

This lemma shows that in principle, any strong (k,ε)-extractor with suitable parameters can be used for privacy amplification. We illustrate this using a construction by Srinivasan and Zuckerman [28] for simplicity, but we point out that using constructions from [29], it is possible to reduce the randomness required for privacy amplification even further. They give an efficiently computable strong (k,ε)-extractor $\mathsf{E} : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ for any k,m,ε with $k \geq m + 2\log 1/\varepsilon + 2$, where $t = 2(k+m) + O(\log n)$. Applying this to a situation where the adversary is given at most $d \geq H_0(Q)$ qubits of storage, we obtain an efficiently computable function $\mathsf{E} : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ which uses only

$$t = 4(d + m + \log 1/\varepsilon + 3) + O(\log n)$$

bits of seed and satisfies $d(\mathsf{E}(X,Y) \leftarrow YQ) \leq \varepsilon$ whenever

$$H_\infty(X) \geq m + 4d + 3\log 1/\varepsilon + 8 \ .$$

For certain parameters, this construction is more efficient in terms of the seed length t than the local extractor described in Corollary V.2.

VII. CONCLUSIONS

While Holevo's celebrated theorem implies that n quantum bits can not be used to store more than n classical bits reliably, this result is in general not applicable in cryptography, where even partial information can make a difference. Indeed, numerous examples are known where quantum bits are more powerful than the same number of classical bits (see e.g., [14, 20, 30, 31]). In this light, it is natural to study the potential advantage offered by quantum information with respect to specific tasks.

We have taken a step in this direction by showing that certain schemes for the bounded storage model which are secure in the presence of classical adversaries are also secure in the presence of adversaries who are in control of

quantum storage. Surprisingly, the corresponding security parameters are almost the same for the quantum and the classical case when only a single bit is extracted. It is straightforward to extend and reformulate this result in terms of communication complexity. It then states that there can not be a large separation between the one-way average-case quantum and classical communication complexities of a boolean function.

This is in sharp contrast to the case of extractors which output several bits. There are extractors that provide security in the classical bounded-storage model, but can not safely be used against quantum adversaries [20]. Nevertheless, it is possible to give a family of constructions that yield secure bits; this is our main contribution.

While our extractors provide security against quantum adversaries, their parameters are far from optimal. Future work can focus on improving these constructions.

APPENDIX A: PROPERTIES OF THE NONUNIFORMITY

We summarize a few properties of the non-uniformity in this section.

The non-uniformity $d(Z \leftarrow W)$ of Z given W can be viewed as the average distance of the conditional distribution $P_{Z|W=w}$ to the uniform distribution, for a random choice of $w \leftarrow P_W$, that is

$$d(Z \leftarrow W) = \mathop{\mathbb{E}}_{w \leftarrow P_W} [d(Z|W=w)] \qquad \text{(A1)}$$

More generally, for a ccq-state ρ_{ZWQ}, where W and Q are not necessarily independent, the non-uniformity of Z given WQ can be written as an average of the corresponding non-uniformities with respect to the conditional states $\rho_{ZQ|W=w}$. This is a direct consequence of Eq. (2). In formula, we have

$$d(Z \leftarrow WQ) = \mathop{\mathbb{E}}_{w \leftarrow P_W} [d(Z \leftarrow Q|W=w)] . \qquad \text{(A2)}$$

In particular, we can write

$$d(\mathsf{E}(X,Y) \leftarrow YQ) = \mathop{\mathbb{E}}_{y \leftarrow P_{\mathcal{U}_\mathcal{Y}}} [d(\mathsf{E}(X,y) \leftarrow Q|Y=y)] ,$$
$$\text{(A3)}$$

where the term in brackets is equal to $d(\mathsf{E}(X,y) \leftarrow Q)$ when Y and Q are independent (which is usually the case in this paper).

Finally, we point out that conditioning on independent random variables leaves the non-uniformity invariant, that is

$$d(Z \leftarrow VQ) = d(Z \leftarrow Q) , \qquad \text{(A4)}$$

if $\rho_{ZQV} = \rho_{ZQ} \otimes \rho_V$. This follows from Eq. (A2).

APPENDIX B: PROOFS OF SECTION II

Proof of Proposition 1. Consider a random variable $\hat{X}$ defined by a channel $P_{\hat{X}|E}$ which takes a value $\hat{x}$ for which $P_{X|E=e}(\hat{x}) = 2^{-H_\infty(X|E=e)}$ with certainty, for every $e \in \mathcal{E}$. Clearly, we have

$$2^{-H_{\mathsf{g}}(X \leftarrow E)} = \Pr[X = \hat{X}] = \mathop{\mathbb{E}}_{e \leftarrow P_E} \left[2^{-H_\infty(X|E=e)} \right] .$$

By Markov's inequality and Eq. (4), this implies that

$$\mathop{\Pr}_{e \leftarrow P_E} \left[H_\infty(X|E=e) \leq H_{\mathsf{g}}(X \leftarrow E) - \log 1/\varepsilon \right] \leq \epsilon .$$

The result then follows by convexity, using the fact that $d(\mathsf{E}(X,Y) \leftarrow YE) = \mathop{\mathbb{E}}_{e \leftarrow P_E} [d(\mathsf{E}(X,Y) \leftarrow Y|E = e)]$ because of Eq. (A1). $\qquad \square$

Lemma 1 can be seen as a special case of Lemma 1′. Their proofs are analogous, but we include both here, as the classical proof is instructive for the quantum generalization.

Proof of Lemma 1. Let $a_{v,w} := 2^{-H_{\mathsf{g}}(X \leftarrow E|V=v,W=w)}$ for all $(v,w) \in \mathcal{V} \times \mathcal{W}$. By definition,

$$a_{v,w} = \sum_{e \in \mathcal{E}} P_{E|V=v,W=w}(e) \max_{x \in \mathcal{X}} P_{X|E=e,V=v,W=w}(x) .$$

In particular,

$$P_{VW}(v,w)a_{v,w} = \sum_{e \in \mathcal{E}} P_{EVW}(e,v,w) \max_{x \in \mathcal{X}} P_{X|E=e,V=v,W=w}(x)$$
$$= \sum_{e \in \mathcal{E}} \max_{x \in \mathcal{X}} P_{XEVW}(x,e,v,w)$$

But by summing over $w \in \mathcal{W}$

$$P_{XEVW}(x,e,v,w) \leq P_{XEV}(x,e,v)$$

and thus

$$P_{VW}(v,w)a_{v,w} \leq P_V(v) \sum_{e \in \mathcal{E}} P_{E|V=v}(e) \max_{x \in \mathcal{X}} P_{X|V=v,E=e}(x)$$

$$= P_V(v) \sum_{e \in \mathcal{E}} P_E(e) \max_{x \in \mathcal{X}} P_{X|E=e}(x)$$

$$= P_V(v)2^{-H_g(X \leftarrow E)}$$

where we used the independence of XE and V in the second step and the definition of $H_g(X \leftarrow E)$ to obtain the last identity. We conclude that

$$\mathop{\mathbb{E}}_{(v,w) \leftarrow P_{VW}} [a_{v,w}] \leq 2^{H_0(W)-H_g(X \leftarrow E)}$$

It is easy to see that

$$\mathop{\mathbb{E}}_{(v,w) \leftarrow P_{VW}} [a_{v,w}] = 2^{-H_g(X \leftarrow VWE)},$$

which proves our first claim. We then use Markov's inequality to obtain

$$\mathop{\Pr}_{(v,w) \leftarrow P_{VW}} \left[a_{v,w} \geq \frac{1}{\varepsilon} 2^{H_0(W)-H_g(X \leftarrow E)} \right] \leq \varepsilon \ ,$$

which is our second claim. $\qquad\square$

Proof of Lemma 1'. By assumption, ρ_{XVWQ} has the form

$$\rho_{XVWQ} = \sum_{(x,v,w) \in \mathcal{X} \times \mathcal{V} \times \mathcal{W}} P_{XVW}(xvw)|xvw\rangle\langle xvw| \otimes \rho_x \ .$$

For every $(v,w) \in \mathcal{V} \times \mathcal{W}$, let $\mathcal{E}^{v,w} := \{E_x^{v,w}\}_{x \in \mathcal{X}}$ be the POVM which maximizes the expression in the definition of $H_g(X \leftarrow Q|V=v, W=w)$. We define the operators $\{F_x^v\}_{x \in \mathcal{X}}$ by

$$F_x^v := 2^{-H_0(W)} \sum_{w \in \mathcal{W}} E_x^{v,w} \ .$$

It is easy to see that $\mathcal{F}^v := \{F_x^v\}_{x \in \mathcal{X}}$ forms a POVM for every $v \in \mathcal{V}$, and the operator inequality $E_x^{v,w} \leq 2^{H_0(W)} F_x^v$ holds. In particular,

$$\mathsf{tr}(E_x^{v,w}\rho_x) \leq 2^{H_0(W)}\mathsf{tr}(F_x^v \rho_x) \qquad (\text{B1})$$

for all $(x,v,w) \in \mathcal{X} \times \mathcal{V} \times \mathcal{W}$. Let us introduce the abbreviation

$$a_{v,w} := 2^{-H_g(X \leftarrow Q|V=v,W=w)} \ . \qquad (\text{B2})$$

for every $(v,w) \in \mathcal{V} \times \mathcal{W}$. By definition and Eq. (B1),

$$a_{v,w} = \sum_{x \in \mathcal{X}} P_{X|V=v,W=w}(x)\mathsf{tr}(E_x^{v,w}\rho_x)$$

$$\leq 2^{H_0(W)} \sum_{x \in \mathcal{X}} P_{X|V=v,W=w}(x)\mathsf{tr}(F_x^v \rho_x) \ .$$

We thus have

$$\mathop{\mathbb{E}}_{(v,w) \leftarrow P_{VW}} [a_{v,w}] \leq 2^{H_0(W)} \sum_{(x,v) \in \mathcal{X} \times \mathcal{V}} P_{XV}(x,v)\mathsf{tr}(F_x^v \rho_x)$$

$$= 2^{H_0(W)} \mathop{\mathbb{E}}_{v \leftarrow P_V} \left[\sum_{x \in \mathcal{X}} P_{X|V=v}(x)\mathsf{tr}(F_x^v \rho_x) \right] \ .$$
$$(\text{B3})$$

But for every $v \in \mathcal{V}$,

$$\sum_{x \in \mathcal{X}} P_{X|V=v}(x)\mathsf{tr}(F_x^v \rho_x) = \sum_{x \in \mathcal{X}} P_X(x)\mathsf{tr}(F_x^v \rho_x)$$

$$\leq 2^{-H_g(X \leftarrow Q)} \qquad (\text{B4})$$

by the assumption that $\rho_{XV} = \rho_X \otimes \rho_V$, and the definition of the latter quantity. Combining Eqs. (B4) with (B3) and (B2) gives

$$2^{-H_g(X \leftarrow VWQ)} = \mathop{\mathbb{E}}_{(v,w) \leftarrow P_{VW}} [a_{v,w}] \leq 2^{H_0(W)-H_g(X \leftarrow Q)} \ ,$$

and the first claim follows. The second claim follows from Markov's inequality, as in the proof of Lemma 1. $\qquad\square$

APPENDIX C: PROOF OF REFINEMENT LEMMA

In the proof of Theorem III.1 we have used the fact that applying classical post-processing after a measurement $\mathcal{F}$ does not increase the non-uniformity. We state this as a lemma; the proof is trivial and follows from the triangle inequality.

Lemma 6. *Let $P_{E|X}$ be a channel, and let $\mathcal{F} := \{F_x\}_{x \in \mathcal{X}}$ be a POVM on $\mathcal{Q}$. Define the operators*

$$E_e := \sum_{x \in \mathcal{X}} P_{E|X=x}(e)F_x$$

for every $e \in \mathcal{E}$. Then $\mathcal{E} := \{E_e\}_{e \in \mathcal{E}}$ is a POVM, and for any cq-state ρ_{ZQ},

$$d(Z \leftarrow \mathcal{E}(Q)) \leq d(Z \leftarrow \mathcal{F}(Q)).$$

Proof. It is trivial to check that $\mathcal{E}$ is indeed a POVM. By definition,

$$d(Z \leftarrow \mathcal{E}(Q)) = \|\rho_{Z\mathcal{E}(Q)} - \rho_{\mathcal{U}_{\mathcal{Z}}} \otimes \rho_{\mathcal{E}(Q)}\|$$

$$= \frac{1}{2} \sum_{(z,e) \in \mathcal{Z} \times \mathcal{E}} \alpha_{z,e} \ , \qquad (\text{C1})$$

where

$$\alpha_{z,e} := \left\| \mathsf{tr}((|z\rangle\langle z| \otimes E_e)\rho_{ZQ}) - \frac{1}{|\mathcal{Z}|}\mathsf{tr}(E_e\rho_Q) \right\| \ .$$

By the definition of E_e and the triangle inequality,

$$\alpha_{z,e} \leq \sum_{x \in \mathcal{X}} P_{E|X=x}(e)\|\mathrm{tr}((|z\rangle\langle z|\otimes F_x)\rho_{ZQ}) - \frac{1}{|\mathcal{Z}|}\mathrm{tr}(F_x\rho_Q)\| \ .$$

Combining this with Eq. (C1) gives the claim. $\qquad\square$

[1] N. Nisan and D. Zuckerman, Journal of Computer and System Sciences **52**, 43 (1996), A preliminary version appeared at STOC '93.

[2] R. Shaltiel, Bulletin of the EATCS **77**, 67 (2002), http://dblp.uni-trier.de.

[3] G. S. Vernam, J. Am. Inst. Elec. Eng. **55**, 109 (1926).

[4] B. Pfitzmann and M. Waidner, Composition and integrity preservation of secure reactive systems, in *7th ACM Conference on Computer and Communications Security*, pp. 245–254, ACM Press, 2000.

[5] R. Canetti, Journal of Cryptology **13**, 143 (2000).

[6] C. H. Bennett, G. Brassard, and J.-M. Robert, SIAM Journal on Computing **17**, 210 (1988).

[7] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Transaction on Information Theory **41**, 1915 (1995).

[8] U. Maurer, Journal of Cryptology **5**, 53 (1992).

[9] Y. Aumann, Y. Z. Ding, and M. O. Rabin, IEEE Trans. on Inf. Theory **48**, 1668 (2002).

[10] S. Dziembowski and U. Maurer, Tight security proofs for the bounded-storage model, in *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, Lecture Notes in Computer Science, pp. 341–350, 2002.

[11] C. Lu, Hyper-encryption against space-bounded adversaries from on-line strong extractors, in *Advances in Cryptology — CRYPTO 2003*, Lecture Notes in Computer Science, pp. 18–22, Springer, 2002.

[12] S. Vadhan, On constructing locally computable extractors and cryptosystems in the bounded storage model, in *Advances in Cryptology — CRYPTO 2003*, Lecture Notes in Computer Science, pp. 61–77, Springer, 2003.

[13] M. Ben-Or, Security of BB84 QKD protocol, Slides available at http://www.msri.org/publications/ln/msri/2002/quantumintro, Part II, 2002.

[14] R. König, U. Maurer, and R. Renner, IEEE Transactions on Information Theory **51**, 2391 (2005), also available at http://arxiv.org/abs/quant-ph/0305154.

[15] R. Renner and R. König, Universally composable privacy amplification against quantum adversaries, in *Second Theory of Cryptography Conference TCC*, , Lecture Notes in Computer Science Vol. 3378, pp. 407–425, Springer, 2005, Also available at http://arxiv.org/abs/quant-ph/0403133.

[16] R. Renner, *Security of Quantum Key Distribution*, PhD thesis, Swiss Federal Institute of Technology (ETH) Zurich, 2005, Also available at http://arxiv.org/abs/quant-ph/0512258.

[17] M. Christandl, R. Renner, and A. Ekert, A generic security proof for quantum key distribution, http://arxiv.org/abs/quant-ph/0402131, 2004.

[18] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, Cryptography in the bounded quantum-storage model, in *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 449–458, IEEE, 2005.

[19] H. Buhrman, M. Christandl, P. Hayden, H. W. Lo, and S. Wehner, On the (im)possibility of quantum string commitment, http://arxiv.org/abs/quant-ph/0504078, 2005.

[20] D. Gavinsky, J. Kempe, and R. de Wolf, Exponential separation of quantum and classical one-way communication complexity for a Boolean function, http://arxiv.org/abs/quant-ph/0607174, 2006.

[21] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, The universal composable security of quantum key distribution, in *Second Theory of Cryptography Conference TCC*, , Lecture Notes in Computer Science Vol. 3378, pp. 386–406, Springer, 2005, Also available at http://arxiv.org/abs/quant-ph/0409078.

[22] R. König, R. Renner, A. Bariska, and U. Maurer, Locking of accessible information and implications for the security of quantum cryptography, http://arxiv.org/abs/quant-ph/0512021, 2005.

[23] S. Wolf, *Information-Theoretically and Computationally Secure Key Agreement in Cryptography*, PhD thesis, Swiss Federal Institute of Technology (ETH Zurich), 1999, ETH dissertation No. 13138.

[24] D. DiVincenzo, M. Horodecki, D. Leung, J. Smolin, and B. Terhal, Phys. Rev. Lett. **92**, 067902 (2004), http://arxiv.org/abs/quant-ph/0303088.

[25] H. Barnum and E. Knill, Journal of Mathematical Physics **43**, 2097 (2002), http://arxiv.org/abs/quant-ph/0004088.

[26] P. Hausladen and W. Wootters, Jour. of Modern Optics **41**, 2385 (1994).

[27] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).

[28] A. Srinivasan and D. Zuckerman, Computing with very weak random sources, in *IEEE Symposium on Foundations of Computer Science*, pp. 264–275, 1994.

[29] O. Reingold, R. Shaltiel, and A. Wigderson, Extracting randomness via repeated condensing, in *IEEE Symposium on Foundations of Computer Science*, pp. 22–31, 2000.

[30] A. Nayak, Optimal lower bounds for quantum automata and random access codes, in *Proceedings of the 40th Annual Symposium on Foundations of Computer Science*, pp. 369–377, 1999, quant-ph/9904093.

[31] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, Dense quantum coding and a lower bound for 1-way quantum automata, in *Proceedings of the 31th ACM Symposium on Theory of Computing*, 1999, quant-ph/9804043.